REMARKS

The Examiner rejected claims 1, 4, 6, 8-12, 15, 17 and 19-20 under 35 U.S.C. 103(a) as being unpatentable over Ahonen (6,976,177).

The Examiner rejected claims 2, 3, 5, 13, 14 and 16 under 35 U.S.C. 103(a) as being unpatentable over Ahonen (6,976,177) in view of Subramaniam et al. (6,640,302).

The Examiner rejected claims 7 and 18 under 35 U.S.C. 103(a) as being unpatentable over Ahonen (6,976,177) in view of Jari et al. (6,907,532).

An Office Action was issued on July 24, 2006 outlining substantially the same rejections as in the current Office Action. In response to that earlier Office Action, Applicant argued that the prior art does not teach or suggest various elements of the claims because Ahonen fails to teach or suggest the use of a shared secret.

The Final Office Action responds to the Applicant's arguments by stating "[t]he Examiner disagrees the shared secret [in Ahonen] is the Security Association (SA), see col. 1, lines 45-67" and "[t]he Examiner disagrees with argument, and notes again the shared secrets are the SAs, which due incorporate certificates."

Applicant respectfully submits that there appears to be some confusion regarding the term "shared secret," as that term cannot possibly refer to a security association. "Shared secret" is a term known in the art and refers to a type of authentication, similar to a password. For the Examiner's reference, a copy of a knowledge base article defining a shared secret is provided attached to this response. Additional evidence can be provided upon the Examiner's request. There are of course numerous different types of authentications, including passwords, shared secrets, and certificates. Each of these types of authentications are different from each other and perhaps more importantly, each of them is different than a security association. A security association is a mapping of certain agreed-upon parameters with two or more entities that will share the parameters. It is essentially an agreement between two or more network entities to use certain settings, protocols, etc. for communication. An authentication is something that is used to authenticate the user or device that will be used in a security association, but equating a

security association with a shared secret is no more correct than equating a security association with a password. They are simply different types of entities.

In Ahonen, certificates are utilized to create multiple security associations. The certificates are the authentications and the security associations are the end goals of the authentication process. A shared secret can only refer to a type of authentication and not to an end goal of an authentication process. As such, Applicant respectfully submits that the Examiner has misunderstood the meaning of the term "shared secret" and respectfully requests that the rejections be reconsidered and withdrawn.

Specifically, claim 1 contains the following elements that cannot be taught by a reference lacking a shared secret: "establishing a correspondence between the IP address and a first shared secret authorized for the user," "receiving a second request from the user to form a virtual private network tunnel, the request incorporating a second shared secret," "determining whether the first shared secret matches the second shared secret," and "forming the virtual private network tunnel when the first shared secret matches the second shared secret."

Furthermore, even if one were to accept the Examiner's position that the security associations in Ahonen are shared secrets, Ahonen would still fail to teach or suggest "determining whether the first shared secret matches the second shared secret; and forming the virtual private network tunnel when the first shared secret matches the second shared secret." The Examiner cites col. 9, line 52 through col. 10, line 7 and col. 1, lines 43-47 of Ahonen as allegedly teaching these elements. Col. 9, line 52 through col. 10, line 7, however, describes a process wherein Ahonen compares fields in a certificate with contents of database to determine whether a match is found and then allowing access to a security association if a match exists. There is, however, no comparison made between a first security association and a second security association, which would be a necessary element if, as the Examiner is attempting, the security association is what is being called the shared secret. Indeed, it appears the Examiner is attempting to have it both ways: calling the security associations in Ahonen shared secrets for the first few elements of claim 1, and then switching and calling the certificates the shared secrets for the last few elements of claim 1. Applicant respectfully submits that this is improper.

As to independent claims 12, 19, and 20, these claims contain elements similar to that as described above with respect to claim 1, and as such Applicant respectfully submits that these claims are also in condition for allowance.

Dependent claims 4, 6, 8-11, 15, and 17 are also patentably distinct from the cited references for at least the same reasons as those recited above for the independent claim, upon which they ultimately depend. These dependent claims recite additional limitations that further distinguish these dependent claims from the cited references. For at least these reasons, claims 4, 6, 8-11, 15, and 17 are not anticipated or made obvious by the prior art outlined in the Office Action.

Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. In lieu of a Notice of Allowance, Applicant notes that this response puts the application in a better condition for appeal and respectfully requests that it be considered and entered. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER LLP

/Marc S. Hanish/
Marc S. Hanish
Reg. No. 42,626

P.O. Box 70250
Oakland, CA 94612-0250
408-255-8001